IJCAT – International Journal of Computing and Technology
Volume 1, Issue 1, February 2014
www.IJCAT.org

Proxy Based Content Centric Networking with Packet Loss Avoidance in Adhoc Network

[1] Seenia Francis, [2] Anju John, [3] Divya Jose, [4] Pelja PauL.N

[1, 2, 3, 4] Calicut University

Abstract - Rapid developments in the mobile technology have transformed mobile phones into multimedia devices. Due to these advancements, user created mobile content is on the increase, both in terms of quality and quantity. In addition, content sharing is getting popular in home networks as well as in social community networks. To keep pace with such a movements the new networking topology named as content centric networking (CCN) optimized for content sharing has appeared. Due to mobility of intermediate nodes, connection between two remote nodes fails frequently bringing packet loss problem. Packet loss cause communication delay, throughput degradation and congestion and may even make the network unusable. This paper proposes a new CCN scheme with packet loss avoidance built into it.

Keywords – **Adhoc Network.**

1. Introduction

A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier. The backbone network usually uses cables. Some of the differences between wired and wireless networks are these two types of networks is one uses network cables and one uses radio frequencies. A wired network allows for a faster and more secure connection and can only be used for distance shorter than 2,000 feet. A wireless network is a lot less secure and transmission speed can suffer from outside interference. Although wireless networking is a-lot more mobile than wired networking the range of the network is usually 150-300 indoors and up to 1000 feet outdoors.

Today, various contents are usually hosted by media servers and web portals, and the only way to retrieve contents is to establish an end-to-end connection with them. While the communication pattern in the internet has been evolving since its early days, from client-server model to peer-to-peer networking, and to cloud networking, one significant point has been shown, That is The usage pattern of the internet has become largely content oriented . That is, content consumers do not care where and how to obtain a piece of content moreover, the current internet's connection exchange model leads to a lot of signaling overhead, especially in the case of mobile consumer devices, which introduces a whole range of inefficient energy consumption. So the efficient networking device has been considered by using a radically different approach, namely content-based networking where content queries and data are routed based on content name.

CCN NODE MODEL

CCN is a new communication paradigm that has been designed to substitute the current Internet. When compared to the current TCP/IP communication model, CCN has the following different characteristics:

i) Receiver-centric communication model: Receivers pull information by sending an interest message. At most one data message is delivered in response to an interest.

ii) Hierarchical content naming scheme: CCN does not address specific hosts, but content object itself. Content is given hierarchical names, which is similar to URLs. Interest packets are forwarded by doing longest-prefix Matching at forwarding decision phase.

iii) Cache and forward architecture: Every CCN devices can cache data and use them to serve future requests

CCN communication is driven by the consumers of data. There are two CCN packet types, Interest and Data (Figure 1). A consumer asks for content by broadcasting its interest over all available connectivity. Any node hearing the interest and having data that satisfies it can respond with a Data packet. Data is transmitted only in response to an Interest and consumes that Interest.1 Since both Interest and Data identify the content being exchanged by name, multiple nodes interested in the same content can share transmissions over a broadcast medium using standard multicast suppression techniques.

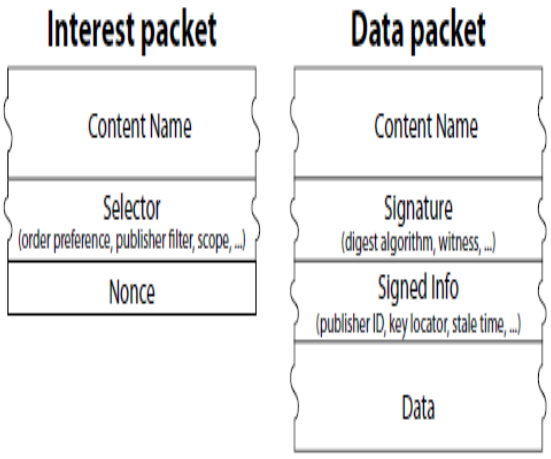


Figure 1 CCN packet types

The FIB is used to forward Interest packets toward potential source(s) of matching Data. It is almost identical to an IP FIB except it allows for a list of outgoing faces rather than a single one. This reflects the fact that CCN is not restricted to forwarding on a spanning tree. It allows multiple sources for data and can query them all in parallel.

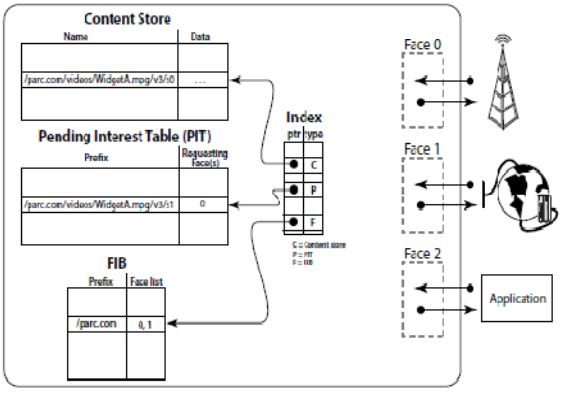


Figure:2 forwarding engine model

2. Related Work

2.1 Proxy-based Mobility Management Scheme in Mobile Content Centric Networking (CCN) Environments

The increase of user generated mobile content raises the need of mobile content sharing. The proxy-based mobility management in CCN environments that can provide low control overhead and low packet loss. The goal of CCN is to create a simple and flexible networking approach that enables network to self-organize and relevant contents where needed.

A CCN node (content requester, CR) asks for contents by sending an Interest packet. Data are then routed the reverse path back to the CR. The CR node has to ask for each segment of the content in the same way. That is, one content is composed of multiple segments. There are too excessive control overheads during content sharing in mobile CCN environments, especially when mobile device is a content requester. That is, when the handoff event happens, a number of redundant Interest packets have to be sent again to retrieve the already-requested Data packets. So, it results in long latency and too much control overhead during node movement.

USER PROXY BASED MOBILE CCN SCHEME

This paper assumes that user proxies with CCN functionality are configured as overlay architecture over IP networks. So, if a user wants to get specific content data, it just sends the content query (Interest) packet to its proxy node. That is, user devices do not need to resolve and make connections with other content holder devices by themselves

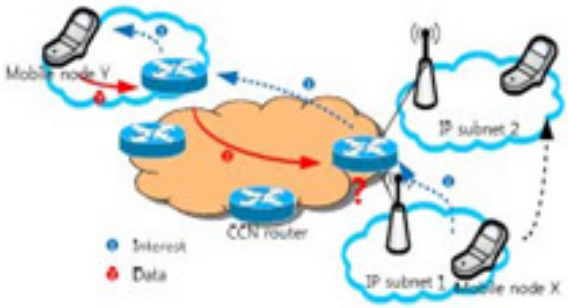


Figure 3

.

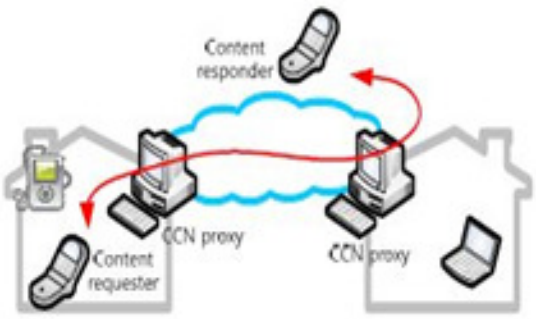


Figure 4

The CCN proxy receiving the Interest packet may try to discover the content itself using normal CCN Interest/Data

exchanges. The proposed proxy-based mobile CCN has the following operation procedures.

Step1. Handover (HO) detection: Mobile node detects when to change network status by the use of physical link information or router advertisements.

Step2. Handover indication: When detecting the handover event is imminent, mobile node sends 'Hold request' message to its proxy node before the actual handover event happens. After receiving 'Hold request' message, the proxy node stops delivering content Data packets to MN's old location and only stores the content data in its local repository for future retransmissions. After that, if a Data packet is received, the proxy node checks whether a specific PIT entry exists. Then, the received content Data packet is not transmitted and just stored at the proxy node's repository. Therefore, the proposed scheme can prevent unnecessary packet losses and network resource consumptions toward the path to old location.

Step3. Handover complete: When acquiring new IP address, the mobile node notifies the new IP address information of its proxy node by using 'Handover notification' message piggybacking the content sequence numbers that it finally received at the old location. The CCN proxy node transmits the stored content data packets toward the new location of mobile node. That is, the proposed scheme does not need to transmit the repeated Interest packets for the stored content data packets.

The advantages are provide lower communication overhead ,provide low control overhead and low packet loss,prevent unnecessary packet transmissions towards old location during handoff.

The disadvantage is long latency and too much control overhead during node movement.

2.2. Proxy-assisted Content Sharing Using Content Centric Networking (CCN) for Resource-limited Mobile Consumer Devices

This paper assumes that user proxies with CCN functionality are configured in overlay architecture over IP networks. The CCN proxy can be either a mobile device or a PC that must be continuously active. The CCN proxy behaves as the common point of routing path for all content sharing. In addition, the proxy serves as a point of indirection (providing relaying services) as well as providing additional services such as message filtering, secure association, and so forth. The basic idea is that user devices ask the proxy to download the requested content on their behalf (as shown in Fig. 5). The CCN proxy participates in the conventional CCN overlay, and takes care of all downloads of the devices. So, if a user device wants to get specific content data, it just sends to its proxy node the content query packet, which is similar with interest packet in original CCN architecture. That is, user devices do not need to resolve and make connections with other content holder devices by themselves.

A. CCN overlay configuration

First of all, a mobile CCN device does a secure association with a CCN proxy node for the content prefix announcement and content sharing. This paper assumes that the proxy nodes configure overlay network in advance and therefore recognizes the identity information of others. Each individual device including proxy nodes carries a unique cryptographic identity in the form of a public key pair. There is a tight coupling between the key pair used by the device and its identity so that all devices can be easily identified. Through the identity information, proxy nodes can establish face configuration to construct routing tables. After the secure association, the mobile CCN device and the proxy node exchange the identity information as well as IP address with each other. Storing such information makes it possible to deliver content data without exchanging additional interest packets when either IP address of mobile consumer device or the serving proxy node is changed. That is, once there is a secure association between a mobile consumer device and one of proxy nodes, there is no further processing at other proxy nodes, except for network association (i.e., to create the face configuration between them).

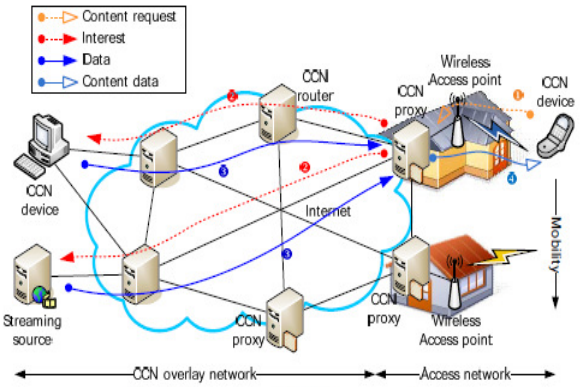


Fig. 5. Proxy-based CCN content sharing

B. Proxy-assisted CCN content sharing

The mobile device that wants to receive a specific content data sends a content request message containing the requested content name to its proxy node

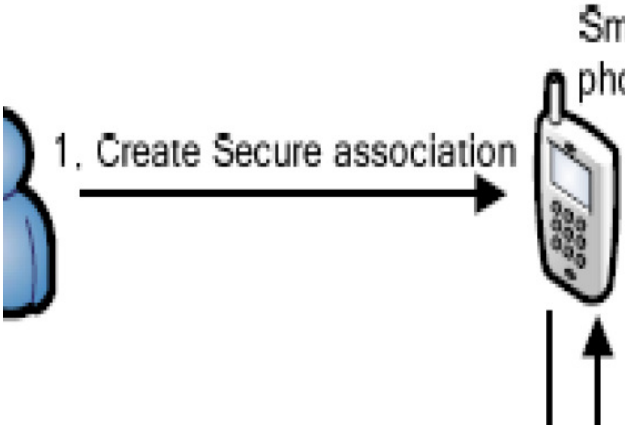


Figure 6

The proxy node receiving the content request message initiates a normal CCN content sharing procedure. That is, the proxy node assumes the content request as one request from its own application layer. After receiving the metadata information of the requested content from content holders, the proxy node delivers the metadata information for the requested content data to the mobile device. It is assumed that the metadata information can be acquired when CCN content is generated and it is piggybacked in the first segment data of the content. So, the mobile device can configure the fake PIT entries for the requesting content data without issuing further interest packets in segment unit of the content data.

The advantage is prevent unnecessary packet transmissions at the previous location that the mobile device already moved out.It can save energy consumption by reducing repeated transmissions of interest packets for data packets not received during network change.

The disadvantage are proxy cost is high,when one proxy failed it is difficult to receive the packet.

2.3 Mobility Management for Mobile Consumer Devices in Content Centric Networking (CCN)

This paper proposes a partial extension based routing update method for mobile content sources in CCN to reduce network convergence time and the number of routing table entry. The proposed scheme starts when a mobile content source (MCS) sends a 'Prefix registration (P Reg)' message to its content router (CR) to inform the movement event. At that time, a MCS locally announces its name prefix to advertise its presence. CRs forward the P Reg message towards the original domain. Through the exchange of PReg messages, the extended path can be configured from the original domain to the operation of a partial path extension (PPx) scheme is largely made of 3 steps. The detailed procedure is as follows.

Step1. Movement indication: When detecting whether to change network status, a MCS sends a P Reg message to announce its presence. Here new domain of MCS to provide seamless reach ability.
Step2. Path extension: The CR receiving a PReg message compares its name prefix domain with that of the PReg message.
Step3. Path update & revocation: In case that the MCS moves away into another prefix domain networks, the previously-established partial route has to be updated.

That is due to the fact that the route reach ability is achieved in a short amount of time through a partial route update that the extended route information is managed only along CRs that constitute the path between the original location and the new one. It can save resource consumption of CCN networking by limiting the range of routing update to the path between the original location and the current location. The proposed scheme has lower amount of overhead comparing with the basic CCN scheme due to its partial route update nature. It keeps this latency more or less constant until it reaches stabilization.

Contrary to client mobility, content source mobility creates a complicated situation: a mobile source requests all relevant content routers to update their routing tables for the successful reception of future/on-going content requests. However, it takes much time to update the routing tables of all content routers. So, interest packets may not reach, if the route to the relevant content source changes; hence the interest packets are unnecessarily sent again because content requesters do not know whether the occurrence of interest retry event is brought about by network problem or node movement. Furthermore, if there are too many mobile content sources, it leads to the pollution of the routing tables for their prefixes, which counters the advantages of prefix aggregation. Consequently, there may be a number of false routing entries in CCN networks and then it leads to unnecessary resource consumption and long communication setup latency.

The advantages are the route reach ability is achieved in a short amount of time through a partial route update that the extended route information is managed only along CRs that constitute the path between the original location and the new one.It can save resource consumption of CCN networking by limiting the range of routing update to the path between the original location and the current location. It keeps this latency more or less constant until it reaches stabilization.The disadvantages are content source

mobility creates a complicated situation. There may be a number of false routing entries in CCN networks.

2.5. CSMA/CN: Carrier Sense Multiple Access with Collision Notification

Under CSMA/CN, the receiver uses PHY-layer information to detect a collision and immediately notifies the transmitter. The collision notification consists of a unique signature, sent on the same channel as the data. The transmitter employs a listener antenna and performs signature correlation to discern this notification. Once discerned, the transmitter immediately aborts the transmission.

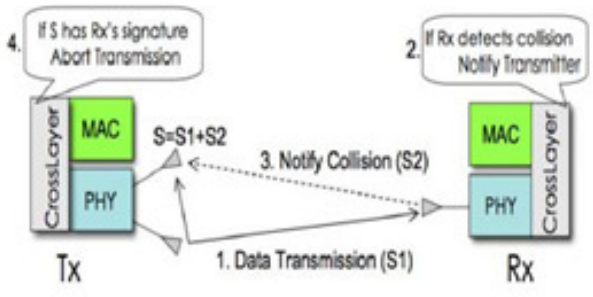


Figure 7

While receiving a packet, the receiver uses physical-layer hints to detect a collision and immediately notifies the transmitter. The transmitter utilizes two antennas: one for normal transmission and another dedicated to listening for the notification. Upon detecting the notification, the transmitter aborts its transmission, freeing up the channel for other transmitters in the vicinity.

The operation of CSMA/CN can be summarized as follows .The transmitter has two interfaces tuned to the same channel, one for transmission and another for listening. The receiver has a single interface (Fig. 1). Once the communication begins, the receiver exploits preamble correlation to detect the presence of an interfering frame. Realizing that the packet reception is likely to fail, the receiver checks the confidence of incoming bits via physical-layer hints from Soft PHY. When the receiver is reasonably confident of an error, it initiates a collision notification to the transmitter. The notification is a short signature unique to the receiver, also known to the transmitter. The transmitter's listening antenna continuously "searches" for this signature using correlation. We show that even in the presence of a strong signal from the transmit antenna, signature correlation at the listening antenna can reliably discern the collision notification. The transmitter aborts, releasing the channel for other nearby transmitters.

In CSMA/CN, the transmitter T uses one interface for transmitting and the other (listener) for listening. The receiver R uses its single interface for multiplexing between transmission and reception. Transmission is initiated as in IEEE 802.11, except one difference: For every packet, the PHY-layer preamble is concatenated with an additional bit sequence, a signature, uniquely computed from the intended receiver's identifier. T ensures the channel is idle and transmits this packet using the transmit antenna. The listening antenna, by virtue of being very close to the transmitting antenna, receives this signal with high signal strength (self-signal). The packet's intended receiver R also receives the transmitted signal and starts decoding the arriving bits. Simultaneously, R initiates collision detection.

Collision happens when a nearby transmitter T1 interferes with R's reception, causing packet corruption. To detect such collisions, receiver R "searches" for a PHY-layer preamble in its incoming signal. Searching occurs through correlation of the preamble with the signal arriving at R's antenna. This happens in parallel and does not affect the normal packet decoding procedure. Once T1's preamble impinges on R's antenna, the correlation exhibits a spike, raising an alert that the packet may be in "trouble." Arrival of a new preamble may not necessarily cause a collision; reception of the packet may be successful sometimes even in presence of the interference. To verify the impact of interference, R consults Soft PHY to obtain confidence values of the bits arriving from T. The confidence value is an indicator of how likely a bit is in error. Based on a window of confidence observations, R infers whether the packet is expected to get corrupted. If so, R halts reception and prepares to send a collision notification to transmitter T. The receiver R searches for a preamble while receiving its frame of interest, but searches for its own signature while receiving an interfering frame.

Upon detecting a collision, R stops receiving and prepares to transmit a collision notification (CN). The CN is composed of only R's own signature. This is the same bit sequence that T included in its packet to R. The receiver transmits the CN packet like a regular 802.11 ACK—there is no carrier sensing, hence the CN is transmitted even though the transmitter is still transmitting. The listening antenna of the transmitter continuously correlates for the receiver's signature in the incoming signal. This correlation is more challenging because the self-signal is much stronger than the notification .We show that even then the listener can discern the notification with consistent accuracy. Upon detecting the collision notification, the listener immediately alerts the transmitting interface, which then suspends the transmission. Once the packet is transmitted, the CSMA/CN receiver responds with an ACK when it is

received correctly. However, unlike 802.11 ACK frame, CSMA/CN ACK is simply a signature. If no ACK signature returns from the receiver, the transmitter times out and retransmit the entire packet.

CSMA/CN is an attempt to approximate CSMA/CD in wireless networks. We show that it is feasible to abort an unsuccessful transmission with the aid of a collision notification from the receiver. Techniques from signal correlation and Soft PHY-based hints are used.

The advantages are wasted transmissions are fewer in CSMA/CN, resulting in better overall throughput. CSMA/CN can detect most of the collisions at all bit rates.

The disadvantages are CSMA/CN cannot be used in conjunction with multiple-input–multiple-output(MIMO).Traffic Conjunction

2.6 An Efficient Automatic Repeat Request Mechanism for Wireless Multihop Relay Networks

Here relay stations are used to forward packets in the networks.. When there are lost packets, relay stations (RSs) decide whether to retransmit these packets with automatic repeat request (ARQ) strategies. An improper ARQ strategy increases latency, blocked packets, and workloads on the multihop relay network. Here a new relay ARQ (RARQ) scheme, providing efficient acknowledgement to reduce packet latency and the number of blocked packets with small workloads.

Compared with conventional single-hop wireless networks, a relay network may suffer more packet losses, thus increasing the overhead for handling packet losses. A conventional way to manage packet losses is to use the automatic repeat request (ARQ) mechanism.

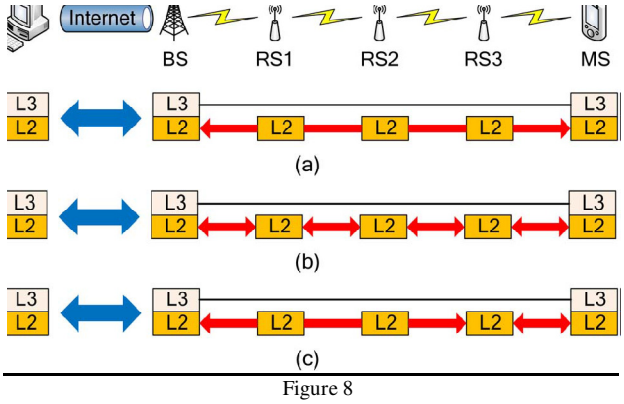


Figure 8

This figure e(a),(b),(c) shows an overview of RARQ scheme

Three conventional relay ARQ (RARQ) schemes that may be applied in the relay network.

(a) The first scheme is the end to -end (E2E) RARQ, in which all RSs simply relay packets, and the error control is delegated to packet senders and receivers.
(b) The second scheme is the hop-by-hop (HbH) RARQ, in which RSs are responsible for detecting errors, sending acknowledgements, and retransmitting packets.
(c) The third scheme is the two-link (TL) RARQ scheme, which divides an E2E path into a multihop relay link and a single-hop access link, and a specific RS has to recover packet losses for both links.

The disadvanteges are relay networks suffer more packet losses.Increase the overhead for handling packet losses.

3. Proposed Scheme

A. Interest Packet Loss Avoidance

During content advertisement, intermediate nodes may receive multiple paths that lead to the source node. In this scheme all nodes keep record of the multiple paths in their FIB tables sorted in terms of hop count and use them to find alternative means to transmit packets. Other metrics instead of hop count may be used. The next two sections describe the two packet loss avoidance options for Interest packet recovery.

1. Alternative Path Selection*:* When an Interest packet arrives on a node, it first checks its cache. If the content is not available in its cache the node then searches in its FIB table for the next hop, with least hop count to destination, and forwards it if it is available. But if the next hop node is marked as unreachable, the node searches its FIB table again and uses the next best available route to the destination.

2. Broadcast: If all alternative next hop nodes are unavailable or there is no alternative path towards the content server, then the node broadcasts the Interest packet with fixed TTL value to prevent flooding. TTL value of two was arbitrarily chosen for this paper's implementation. Because of frequent mobility of nodes and change of topology in wireless networks, new nodes that lie in a path towards the content server but with no path entry in their FIB table may arrive in the vicinity of the current node. This broadcast scheme uses the newly arriving nodes as a bridge to reach nodes in the path to destination server with an existing entry in their FIB table. The nodes that received the broadcast packet first check sequence number and TTL value of the packet. If the TTL value is not zero, the same content request with similar sequence number was not received and the requested content isn't available

in its content store, then the receiving node calculates defer time and starts overhearing. After the defer time expired and confirming that no other node has forwarded the same packet, it decrements its TTL value, checks its routing table and forwards it to next hop if available or broadcasts it otherwise. Sequence number on data packet is used so that any duplicate Interest packets that arrive on a single node are not unnecessarily forwarded more than once.

B. Data packet loss avoidance

In typical CCN when a node receives data packet, it looks up the next hop node in its pending Interest table (PIT) and forwards it. But if the next hop node is unreachable and the link is broken, the node drops the packet and the client will have to wait for its timer to expire before sending its Interest request again.

After detection of link failure that causes data loss, our proposed scheme uses broadcast to reach nodes that may have pending Interest with same content name. Newly arriving nodes or other intermediate nodes will further broadcast the data packet to their neighboring nodes, increasing the probability of reaching nodes that lie in the path of the original Interest request. Similar to Interest packet, the data broadcast packet also has sequence number to prevent duplicate broadcast and fixed TTL value to minimize flooding in the network.

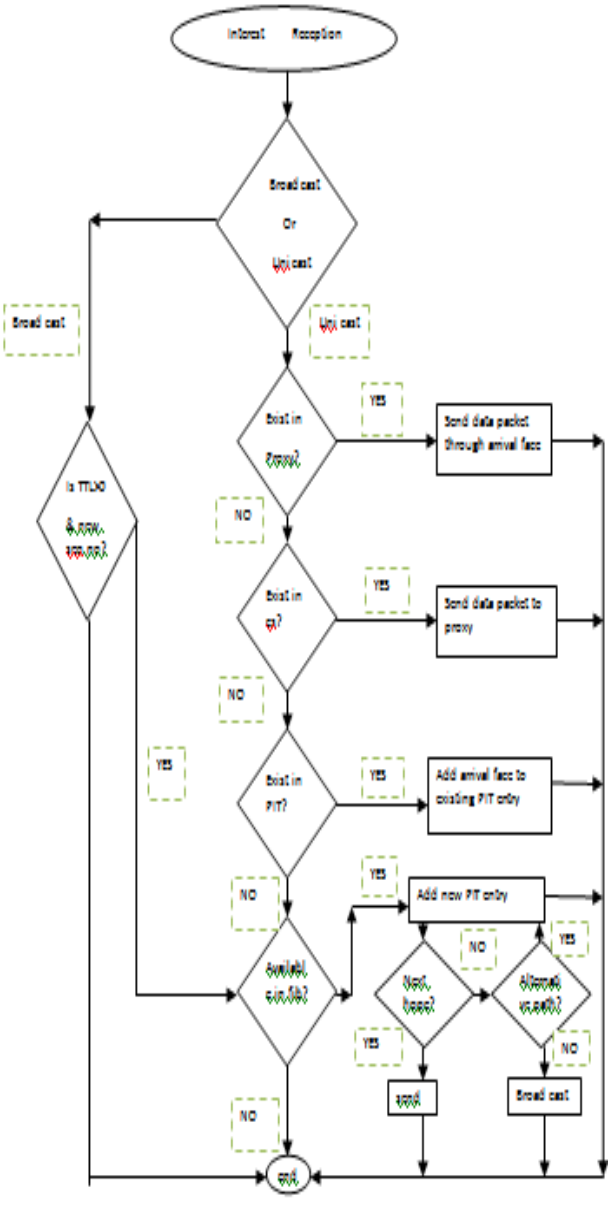
The proposed scheme ensures before transmission that the link with its next hop node is functioning before using it and finds an alternative means. The proposed scheme addresses two mobility scenarios that cause packet loss:

The first scenario is when an intermediate node moves from its previous location. This causes both Interest and Data packet loss. The proposed scheme avoids packet loss by first using alternative path and broadcast. In the case of Data packet, the scheme proposes broadcast since the Data can only follow the path used by its associated Interest packet. Even if the data is not received by the next node in the path of Interest request, it will be cached in the nodes that received the data broadcast and will delivered faster next time it is requested by the client node.

The second scenario is movement of client node. Movement of the client node that requested the data affects delivery of data. The client will receive the data using broadcast if it has not moved more than two hops away from its preceding node. Even if it is more than two hops away, the next time it requests the data, it will receive it from nearby node since the broadcasted data packet will be cached by the nodes in the data broadcast.

C. Movement indication

A mobile device detects when to change network status by using physical link information or subnet address. In the proposed architecture, both subnet change and proxy change are considered to be a handoff event. As the proposed scheme Content data packet towards mobile devices. Content requester is directly related with the new



face**.** Configuration of CCN architecture to the proxy node. In the same manner, the proxy change event should be notified to the previous proxy node to prevent unnecessary packet loss and resource consumption. When detecting that the movement event is imminent, the mobile device

sends 'Hold request' message to a current proxy node. After receiving the 'Hold request' message, the current proxy node stops delivering content data packets toward the mobile device and only stores the content data in its local repository for subsequent retransmissions. For that, the HO field of the relevant entry in PIT is set to 1. As shown in Fig. 7, 8 the CCN proxy node receiving interest packet that indicates specific.

Content data configures content based routing entry for future content data delivery. That is, the routing table architecture of the proposed scheme has only difference in the 'HO' field of PIT configuration.

D. Prefix registration

(PReg) message -client node sends a prefix Registration message to it's proxy to inform the movement event.

E. Acknowledgement

When client node received data packet correctly, client node sends an ack to proxy node delete the data and delete the PIT entry.

F. Collision Notification

While receiving the packet the receiver uses physical layer information to detect a collision and immediately notifies the transmitter by a negative acknowledgement. Where getting NACK,the proxy node retransmit the packet to the client node.

In this scheme, mobile nodes detect availability of neighbouring nodes using periodic overhearing of their activities. If a neighbouring node fails to forward periodic advertisement or it is inactive for some fixed time, the link between the two nodes is considered to be unavailable. The packet loss avoidance scheme begins when a connection between two nodes is detected to be broken this way. In the typical CCN, a node receiving an Interest packet searches its FIB table for next hop entry. The content provider sends the requested data by following the reverse path of the Interest packet used. If the packet is not received successfully, it will be dropped and the intermediate sender doesn't take any prior action to avoid occurrence of packet loss. The original node that requested the packet will have to wait for some timeout value to retransmit its requested interest packet Flow chart of the proposed scheme's packet

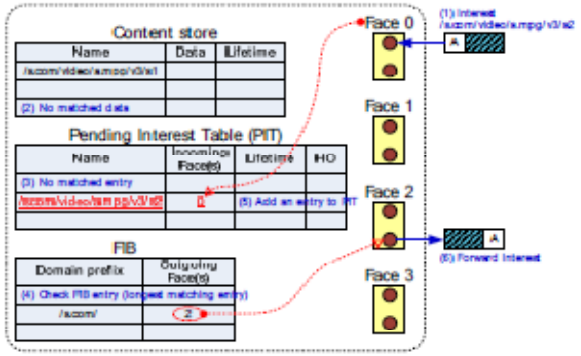


Fig. 7. Interest packet processing at proxy CCN device

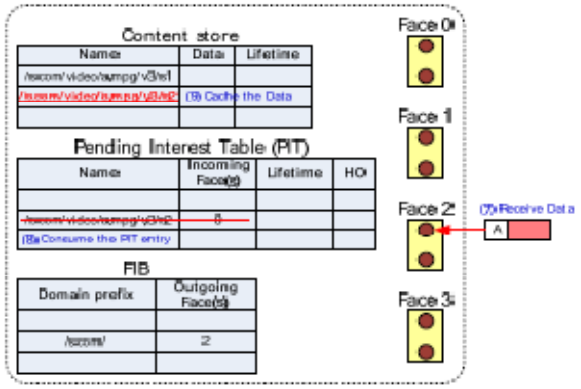


Fig. 8. Modified content data processing at proxy CCN device during handover

processing, Interest packet processing starts by checking whether the packet is broadcast or uncast. If it is broadcast, it checks its TTL value and sequence number and passes it to the typical CCN's function of searching entry in FIB table, otherwise it will drop it. If a next hop entry is available for the content and there is no cached content, it sends the packet using the best available route available. If there is no next hop node, it calculates differ time, listen its neighbours until timer expires and broadcasts it only if no neighbour already sent similar packet. The unicast packet processing follows similar procedure, except that it doesn't need to check TTL value. In data packet processing in our scheme. The additional features in this scheme are that before deciding to send the data to its next hop node, the current node makes sure its neighbour node is available. If it is available it proceeds similar to the typical CCN, otherwise it broadcasts the packet setting TTL value of two and sequence number. In our proposed scheme include backtracking and acknowledgement can be provided to know whether the data is received or not.

The following section explains the proposed scheme for recovering Interest and Data packet loss because of link failure.

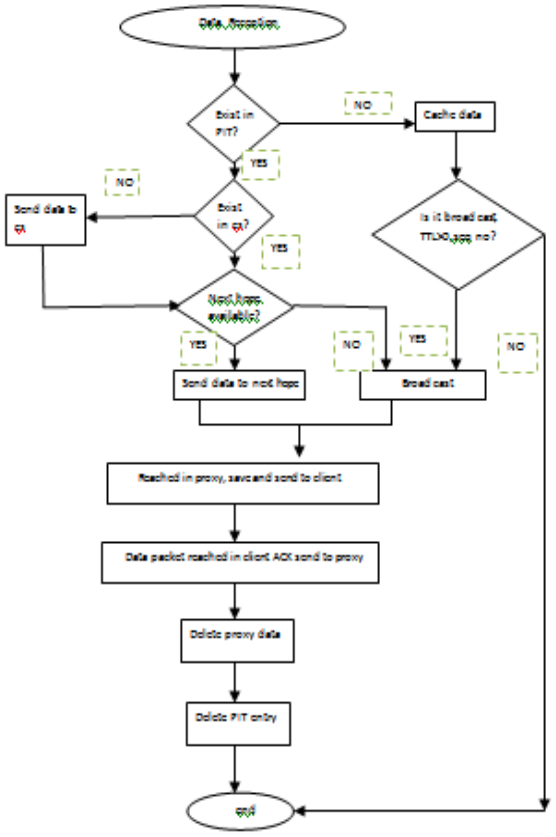
4. Performance Evaluation

A. Simulation Environment

We used content centric network as defined by using proactive routing update to populate its FIB table entry and implemented using OPNET simulator. Our scheme was also implemented using OPNET and compared it with the typical CCN. We compared typical CCN and our proposed scheme using four parameters, namely delivery ratio, round trip time, cache hit ratio and prefix announcement interval time variation. We used 15 seconds as an interval period for prefix announcement by the content server for the first three parameters. Table1 shows the other parameters used in the simulation environment.

B. Result Analysis

Fig 9 depicts successful delivery ratio of packets measured by varying node mobility speed from 0 to 20 m/s. Delivery ratio is a ratio of how much of the packets requested by a client node are delivered successfully.



As shown in Fig 9, the proposed scheme outperforms the typical CCN. Initially at stable state, the typical CCN performs slightly better than our scheme The reason for that slight under performance is the usage of overhearing causes false positive assumption of link breakage even if the nodes are stable and the possibility of link failure is low. That causes a node to use less optimal alternative path or broadcast even if the best path is available. But when we increase node mobility speed, the advantage our scheme has over typical CCN becomes obvious and grows to as much as 13% difference at 20m/s speed..

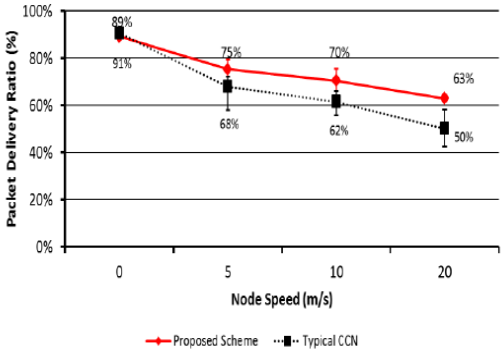


Fig . 9. Packet Delivery Ratio varying Node Speed

The second parameter used to examine the proposed scheme is round trip time (RTT). The RTT is calculated only for the successfully delivered user requested data. It is an average time of all successfully served requests. Data requests that were not delivered are not included in the average RTT value. As shown in fig 10, the proposed scheme consistently has higher RTT than typical CCN. The proposed scheme has higher RTT value since, at the event of link failure, the Data or Interest packets are sent through alternate paths broadcast that generally take more time than the original path. In the case of typical CCN, the lost Interest or Data packets are not included in the average RTT calculation since they are not successfully delivered to the user. The more speed the nodes have the better our proposed scheme performs, since there is more link failure in higher speed.

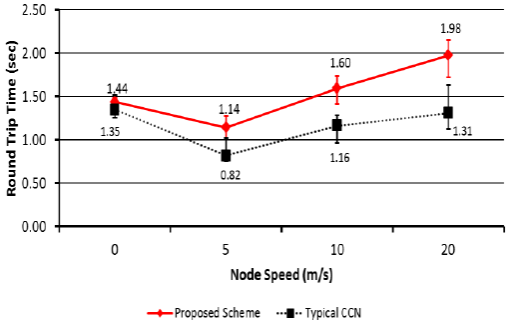


Fig 10. Round Trip Time varying Node Speed

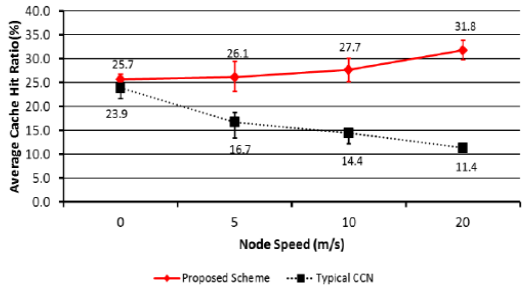


Fig 11. Average Cache Hit Ratio varying Node Speed

Figures 11 show the performance metric in terms of average cache hit. Consumers are randomly selected among the mobile nodes in the simulated grid and the speed of the nodes was kept between 0 to 20 m/sec increasing in linear fashion. Advantage of the proposed scheme becomes less visible due to effect of overhearing and the subsequent use of alternate paths between the nodes when the network is stable. Caching performance difference between our proposed scheme and typical CCN becomes more visible with increase of speed of nodes, going as much as 20% improvement. With increasing speed of the cache hit performance, our approach starts to increase whereas in typical CCN the performance degrades. When the nodes in a network increase their speed, there will be more link failure and hence more packet loss in the network.

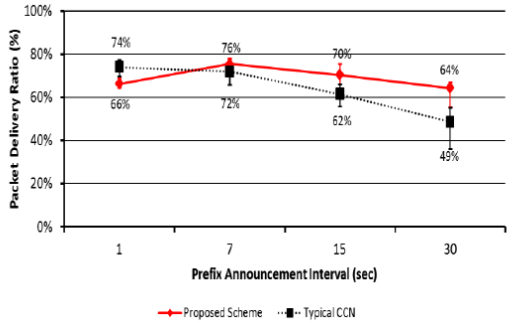


Fig 12. Packet delivery ratio with packet announcement period variation

Figure 12 shows packet delivery ratio by varying content provider's prefix announcement rate. We started with a constant node mobility speed of 10 m/sec, a prefix announcement rate of 1 advertisement per 1 second and increased it linearly up to 1 advertisement per 30 seconds. The result in the graph shows that under heavy prefix advertisement scenario of 1 advertisement per 1 second the typical CCN performs better by sacrificing the network performance due to heavy traffic being generated by the content announcements. As we lower down the advertisement interval gradually, we can clearly see that our approach starts to perform better due to the fact that in a high mobility environment low content announcements result in stale FIB entries that don't reflect the recent network setup. Hence typical CCN fails to forward packets successfully since it is dependent on this stale FIB table. But our proposed scheme recovers the failed links and makes use of the newly arriving nodes to forward packets to destination.

5. Conclusion

In this paper, we developed a new content-centric link recovery scheme that improves content retrieval, caching, and delivery in MANETs. The typical CCN implementation waits for the client node that sent the interest packet to detect packet loss, which increases transmission delay and degrades throughput on the network. Our proposal is designed to cope with the wireless link impairments and highly dynamic topologies and to limit the signaling overhead. Our proposed scheme recovers lost packets by detecting the disconnected node and trying alternative means to successfully transmit data or interest packets. The link recovery is transparent to the consumer and is performed without using any additional control messages, which add overhead on the network.

Reference

[1] Van Jacobson et al. "Network Named Content," in ACM, 2009.

[2] Soon Y. et al. "CCN in Tactical and Emergency MANETs," in Wireless Days Conference, Venice, Italy, 2010

[3] Michael et al. "Listen First Broadcast Later: Topology-Agnostic Forwarding under High Dynamics" Technical Report 100021, UCLA Computer Science Department, 2010.

[4] Marica et al. "CHANET: A Content-Centric Architecture for IEEE 802.11 MANETs," Network of the Future, 2011

[5] David B. et al. "DSR: The Dynamic Source Routing Protocol for Multi- Hop Wireless Ad Hoc Networks", Carnegie Mellon University

[6] Perkins CE. et al. "Ad-hoc On-Demand Distance Vector Routing," AMCSA '99

[7] Marina et al. "On-demand Multipath Distance Vector Routing for Ad- hoc Networks," Proc. of 9th IEEE Int. Conf. On Network Prot., 2001

[8] Charles E, Pravin Bhagwat "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, " SIGCOMM 94 London England UK

[9] Jerry Wang et al. " OLSR-R3: Optimized Link State Routing with Reactive Route Recovery, " in APCC, Shanghai, China, October 2009